

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-269078

(43)Date of publication of application : 09.10.1998

(51)Int.Cl.

G06F 9/06
G06F 9/06
G06F 9/445
G06F 13/00
G06F 17/60

(21)Application number : 10-009479

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 21.01.1998

(72)Inventor : TAKAHASHI TOSHINARI

(30)Priority

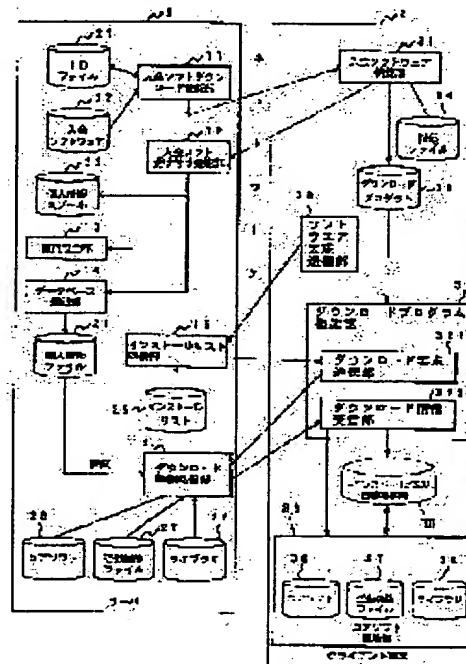
Priority number : 09 8867 Priority date : 21.01.1997 Priority country : JP

(54) SOFTWARE DISTRIBUTION METHOD, SERVER DEVICE AND CLIENT DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To enable a user to use and settlement of account of software in a safe and simple way, by transmitting previously an install list of software via a software provider and interpreting the list before it is downloaded by a personal computer, etc., of the user.

SOLUTION: The software provider previously transmits an install list of software, and this list is interpreted before it is downloaded by a personal computer, etc., of a user. At the same time, an install list transmission part 15 of a server 1 that received a software transmission request from the user reads the install list corresponding to the designated one out of an install list store part 25 and sends it to a client terminal 2. A download program function part 32 of the terminal 2 receives the install list and processes it via a download request transmission part 321. Then the part 43 transmits the download request selected based on the install list to the server 1.



LEGAL STATUS

[Date of request for examination]

12.09.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

This Page Blank (uspto)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-269078

(43) 公開日 平成10年(1998)10月9日

(51) IntCl⁶

G 0 6 F 9/06

識別記号

5 5 0

F I

G 0 6 F 9/06

5 5 0 Z

5 5 0 A

4 1 0 P

3 5 1 H

4 2 0 J

9/445

13/00

13/00

4 1 0

3 5 1

9/06

審査請求 未請求 請求項の数11 O L (全 16 頁) 最終頁に続く

(21) 出願番号

特願平10-9479

(22) 出願日

平成10年(1998)1月21日

(31) 優先権主張番号

特願平9-8867

(32) 優先日

平9(1997)1月21日

(33) 優先権主張国

日本 (J P)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 高橋 俊成

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

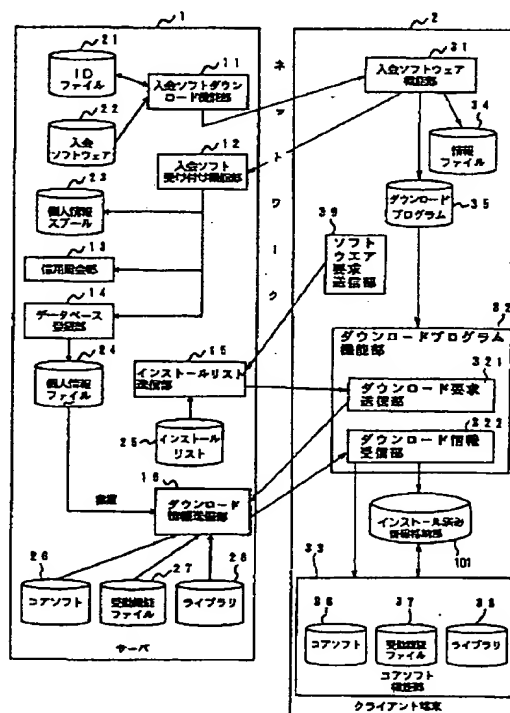
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 ソフトウェア流通方法およびサーバ装置およびクライアント装置

(57) 【要約】

【課題】 ユーザが安全かつ簡便にソフトウェアの利用および決済が行えるソフトウェア流通方法を提供する。

【解決手段】 ソフトウェア提供者が指定されたソフトウェアをネットワークを介して利用者に提供するソフトウェア流通方法において、利用者側の装置からソフトウェア要求をソフトウェア提供者へ送信し、それにより指定されたソフトウェアに対応した複数のファイルのインストール情報をソフトウェア提供者側の装置から前記利用者へ送信し、利用者側の装置が、前記複数のインストール情報を参照して要求すべきファイルを選択し、この選択したファイルを要求するためのダウンロード要求を前記ソフトウェア提供者へ送信し、ソフトウェア提供者側の装置から、前記ダウンロード要求に示されるファイルを含むダウンロード情報を送信し、それに従い利用者側の装置が前記ファイルのインストールを行う。



【特許請求の範囲】

【請求項1】 ソフトウェア提供者が指定されたソフトウェアをネットワークを介して利用者に提供するソフトウェア流通方法において、

利用者側の装置から、指定するソフトウェアの提供を要求するためのソフトウェア要求をソフトウェア提供者へ送信し、

ソフトウェア提供者側の装置から、前記ソフトウェア要求により指定されたソフトウェアに対応した複数のファイルのインストール情報をまとめて前記利用者へ送信し、

利用者側の装置が、前記複数のインストール情報を参照して要求すべきファイルを選択し、この選択したファイルを要求するためのダウンロード要求を前記ソフトウェア提供者へ送信し、

ソフトウェア提供者側の装置から、前記ダウンロード要求に示されるファイルを含むダウンロード情報を送信し、

利用者側の装置が、前記ダウンロード情報に従って前記ファイルのインストールを行うことを特徴とするソフトウェア流通方法。

【請求項2】 ソフトウェア提供者側の装置と利用者側の装置は、ソフトウェア提供者と利用者として共有される共有鍵を記憶し、

利用者側の装置は、前記ダウンロード要求をこの共有鍵に関連付けて送信し、

ソフトウェア提供者側の装置は、前記ダウンロード要求の正当性を自装置の記憶する共有鍵を用いて検査した後に、前記ダウンロード情報を送信することを特徴とする請求項1に記載のソフトウェア流通方法。

【請求項3】 ソフトウェア提供者側の装置と利用者側の装置は、ソフトウェア提供者と利用者として共有される共有鍵を記憶し、

ソフトウェア提供者側の装置は、前記ダウンロード情報をこの共有鍵に関連付けて送信し、

利用者側の装置は、前記ダウンロード情報の正当性を自装置の記憶する共有鍵を用いて検査した後に、前記ファイルのインストールを行うことを特徴とする請求項1に記載のソフトウェア流通方法。

【請求項4】 利用者側の装置は、ソフトウェア要求を送信する際に、当該ソフトウェアのインストールに関連する利用者側の環境判定結果を併せて送信し、

ソフトウェア提供者側の装置は、この環境判定結果に応じて内容の異なる、複数のインストール情報を送信することを特徴とする請求項1に記載のソフトウェア流通方法。

【請求項5】 ソフトウェア提供者から提供されるソフトウェアは、単独で動作可能な能動機能部と、この能動機能部に組み込まれて動作可能となる受動機能部とから構成され、

ソフトウェア提供者側の装置は、利用者からのダウンロード要求に示されるファイルに前記受動機能部に対応するファイルが含まれる場合に、該受動機能部に対応するファイルについて課金を行い、前記能動機能部に対応するファイルについては無料で提供することを特徴とする請求項1に記載のソフトウェア流通方法。

【請求項6】 ソフトウェア提供者側の装置と利用者側の装置は、ソフトウェア提供者と利用者として共有される共有鍵を記憶し、

10 ソフトウェア提供者側の装置は、送信しようとするダウンロード情報に有料部分が含まれる場合には、この共有鍵を用いて該ダウンロード情報の有料部分もしくは全部を暗号化して送信し、

利用者側の装置は、前記ダウンロード情報を自装置の記憶する共有鍵を用いて復号化してインストールを行うことを特徴とする請求項1に記載のソフトウェア流通方法。

【請求項7】 ソフトウェア提供者側の装置と利用者側の装置が記憶する共有鍵は、利用者のソフトウェア料金の決済に関わる識別情報との対応付けが保証された共有鍵であることを特徴とする請求項2または3または6に記載のソフトウェア流通方法。

【請求項8】 ソフトウェア提供者側の装置は、1つのファイルを分割して複数のダウンロード情報として提供する場合に、このファイルのインストール情報に分割に関する情報を含めて送信することを特徴とする請求項1に記載のソフトウェア流通方法。

【請求項9】 利用者側の装置に設けられた、前記ダウンロード要求を送信するためのプログラム、および、前記ダウンロード情報に従ってインストールを行うためのプログラムのうちの少なくとも一方は、それ自体のバージョン情報を持ち、

ソフトウェア提供者側の装置は、複数のインストール情報を送信する際に、利用者側のこれらのプログラムに推奨されるバージョン情報を併せて送信し、

30 利用者側の装置は、前記ダウンロード要求の送信もしくは前記インストールに先立ち、利用者側のこれらのプログラム自身のバージョンアップに必要な情報をソフトウェア提供者に要求することを特徴とする請求項1に記載のソフトウェア流通方法。

【請求項10】 指定されたソフトウェアをネットワークを介してクライアント端末に提供するサーバ装置において、

クライアント端末から受信したソフトウェア要求により指定されたソフトウェアに対応した複数のファイルのインストール情報を記述したインストールリストを、該クライアント端末がこれら複数のファイルのうち必要なものを選択できるように、該クライアント端末へ送信するインストールリスト送信手段と、

50 クライアント端末が選択した必要なファイルを示すダウ

ンロード要求を受信し、このダウンロード要求に示されるファイルを含むダウンロード情報を、該クライアント端末がこのダウンロード情報に従って該ファイルをインストールできるように、該クライアント端末へ送信するダウンロード情報送信手段とを具備したことを特徴とするサーバ装置。

【請求項11】 ネットワークを介してサーバから提供されたソフトウェアを利用するクライアント装置において、

指定するソフトウェアの提供を要求するためのソフトウェア要求を、サーバへ送信するソフトウェア要求送信手段と、

このソフトウェア要求の指定するソフトウェアに対応した複数のファイルのインストール情報が記述されたインストールリストをサーバから受信し、この受信したインストールリストを参照して要求すべきファイルを選択し、この選択したファイルを要求するためのダウンロード要求を該サーバへ送信するダウンロード要求送信手段と、

このダウンロード要求の示すファイルを含むダウンロード情報をサーバから受信し、この受信したダウンロード情報に従って前記ファイルのインストールを行うダウンロード情報受信手段とを具備したことを特徴とするクライアント装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ソフトウェア流通システムに関する。

【0002】

【従来の技術】計算機および計算機ネットワークが普及し、ソフトウェアの流通は現金などを用いた従来の取引形態によらずとも、全て電子的に行うことができるようになった。

【0003】今日では、インターネットの急速な普及に伴って、プログラムなどの情報を電子的に配布し課金するシステムが広く行われている。インターネット等のネットワークを介してのソフトウェアの流通に必要とされる主な要求課題としては、(1)ソフトウェアを入手しようとする人が誰であるかを特定し安全に課金を行うこと(高いセキュリティ性)、(2)ソフトウェアは比較的容易にコピー(複製)を作成することのできるため、その対応策であるソフトウェアの著作権の保護(違法コピーの防止)、(3)ウイルスを含んだソフトウェアの蔓延への取り組み等がある。

【0004】従来、計算機ネットワーク上での課金のメカニズムは、暗号技術に基いた認証技術が用いられてきた。例えば、計算機ネットワークを使ってクレジットカード番号を伝える場合、通信回線を盗聴することによって他人がクレジットカード番号を盗めるのでは困るから、クレジットカード番号を暗号化して転送するように

なっていた。

【0005】また、違法コピー防止の方法も考えられてきた。最も良く使われる方法は、ソフトウェアに何らかの暗号化を施し、データを復号する鍵(暗号鍵やパスワードなど)を持っている人だけが内容を知ることができる方法である。しかし、この方法によっても、パスワード自体を違法にコピーすることによって、ソフトウェアの違法コピーが可能となってしまう。

【0006】また、ネットワークを介してプログラム等の情報交換を行うわけであるからウイルスを含んだソフトウェアの蔓延への取り組みは不可欠である。さらに、ネットワークを介して大容量の情報を送信するわけであるから回線費用等も考慮して通信資源の有効利用を考慮する必要もある。

【0007】ユーザの利便性を考慮すれば、ネットワークを介してプログラム等をダウンロードして、それを自端末にインストールする等の操作はパソコンの扱いに不慣れな者にとって酷である。このようなシステムを広く普及させるためには、パソコン、通信等の知識がなくとも簡単に操作できるような仕様であることが要求されるであろう。

【0008】また ネットワークを介しての電子的情報の販売においては、購入した製品に不満があった場合に返品が不可能であるため、その対策も必要である。また、ネットワークを介してソフトウェアのバージョンアップへの対応が容易に行えるようであれば、ユーザの販売者への信頼が高まり購入意欲を高め、システムの普及も図れるであろう。

【0009】

【発明が解決しようとする課題】このように、従来のソフトウェア流通システムは、ユーザの利便性、ネットワークのレスポンス、ソフトウェアの違法コピー等に対しては充分に配慮されていないという問題点があった。

【0010】本発明は、ネットワークを介して提供されるソフトウェアの購入要求指示、インストール、頻繁に起こるソフトウェアのバージョンアップ等のさまざまな手続きを簡潔に設定し、ユーザが安全かつ簡便な方法でソフトウェアの利用および決済が行われることを可能とするソフトウェア流通システムを提供することを目的とする。

【0011】

【課題を解決するための手段】

(1)本発明のソフトウェア流通方法は、ソフトウェア提供者が指定されたソフトウェアをネットワークを介して利用者に提供するソフトウェア流通方法において、利用者側の装置から、指定するソフトウェアの提供を要求するためのソフトウェア要求をソフトウェア提供者へ送信し、ソフトウェア提供者側の装置から、前記ソフトウェア要求により指定されたソフトウェアに対応した複数のファイルのインストール情報をまとめて前記利用者へ

送信し、利用者側の装置が、前記複数のインストール情報を参照して要求すべきファイルを選択し、この選択したファイルを要求するためのダウンロード要求を前記ソフトウェア提供者へ送信し、ソフトウェア提供者側の装置から、前記ダウンロード要求に示されるファイルを含むダウンロード情報を送信し、利用者側の装置が、前記ダウンロード情報に従って前記ファイルのインストールを行うことを特徴とする。

【0012】本発明によれば、ソフトウェア提供者（サーバ）から複数のファイルのインストール情報（例えばインストールリスト）が送られるため、この中から利用者側の装置（クライアント端末）が自動的に必要なものを選択し、必要なものだけをサーバに要求することが可能となる。そして、サーバから送られるダウンロード情報（要求したファイルの他に例えばインストールの仕方などが含まれていてもよい）に従って必要なファイルをインストールする。

【0013】インストール情報には、例えばファイル名が含まれ、既に利用者側に存在するファイル以外のものを自動的に要求することができる。したがって、同じファイルを二度ダウンロードしてしまい、結果的に二重に課金されてしまうようなことを、ユーザの手を煩わせることなく、防ぐことができる。

【0014】また、インストール情報には、例えばファイルのバージョン情報が含まれていてもよく、既に利用者側に存在するバージョンより新しいバージョンのものを自動的に要求することができる。

【0015】また、インストール情報には、例えばファイルのサイズの情報が含まれていてもよく、利用者側の装置の記憶容量にそのファイルが格納できるだけの余裕があるファイルに限って要求するようなこともできる。

【0016】（2）ソフトウェア提供者側の装置と利用者側の装置は、ソフトウェア提供者と利用者で共有された共有鍵を記憶し、利用者側の装置は、前記ダウンロード要求をこの共有鍵に関連付けて送信し、ソフトウェア提供者側の装置は、前記ダウンロード要求の正当性を自装置の記憶する共有鍵を用いて検査した後に、前記ダウンロード情報を送信するようにしてもよい。

【0017】こうすると、サーバは、ダウンロード要求の正当性（例えばソフトウェア料金の決済ができるユーザ本人からの要求であること）が確認された場合にのみダウンロードを許すようなことができる。

【0018】（3）ソフトウェア提供者側の装置と利用者側の装置は、ソフトウェア提供者と利用者で共有された共有鍵を記憶し、ソフトウェア提供者側の装置は、前記ダウンロード情報をこの共有鍵に関連付けて送信し、利用者側の装置は、前記ダウンロード情報の正当性を自装置の記憶する共有鍵を用いて検査した後に、前記ファイルのインストールを行うようにしてもよい。

【0019】こうすると、クライアント端末は、正当な

サーバからのダウンロード情報である（例えばウイルスが混入していないと判断できる）と確認された場合にのみインストールを実行するようなことができる。

【0020】（4）利用者側の装置は、ソフトウェア要求を送信する際に、当該ソフトウェアのインストールに関連する利用者側の環境判定結果（例えばクライアント端末のOSが何であるかなど）を併せて送信し、ソフトウェア提供者側の装置は、この環境判定結果に応じて内容の異なる、複数のインストール情報を送信するようにしてもよい。

【0021】（5）ソフトウェア提供者から提供されるソフトウェアを、単独で動作可能な能動機能部と、この能動機能部に組み込まれて動作可能となる受動機能部から構成し、ソフトウェア提供者側の装置は、利用者からのダウンロード要求に示されるファイルに前記受動機能部に対応するファイルが含まれる場合に、該受動機能部に対応するファイルについて課金を行い、前記能動機能部に対応するファイルについては無料で提供するようにすることも有効である。

【0022】これによれば、例えばまずソフトウェアの試供版を能動機能部としてユーザに無料で提供し、ユーザがそれを気に入れば正規の製品としての機能を実現するための受動機能部を有料で提供することができる。

【0023】（6）本発明において課金を行うために、ソフトウェア提供者側の装置と利用者側の装置は、ソフトウェア提供者と利用者で共有された共有鍵を記憶し、ソフトウェア提供者側の装置は、送信しようとするダウンロード情報に有料部分が含まれる場合には、この共有鍵を用いて該ダウンロード情報の有料部分もしくは全部を暗号化して送信し、利用者側の装置は、前記ダウンロード情報を自装置の記憶する共有鍵を用いて復号化してインストールを行うようにしてもよい。このとき、ソフトウェア提供者側の装置と利用者側の装置が記憶する共有鍵は、利用者のソフトウェア料金の決済に関わる識別情報との対応付けが保証された共有鍵であることが好ましい。

【0024】このようにすれば、提供するソフトウェアのうち少なくとも有料部分のファイルは、クライアント端末にダウンロードされると暗号化されたまま格納され、サーバと共有された共有鍵を持っていない限り復号化できない。

【0025】（7）そして、この共有鍵をあらかじめ料金決済に関わる識別情報との対応付けが保証されたものとしておけば、ソフトウェア購入の都度セキュリティ性の高いクレジットカード番号等をクライアントからサーバへ送信する必要がなくなり、安全性が確保される。

【0026】なお、上記の共有鍵を、クライアント端末毎に一義的に定められるコード情報に基づいて暗号化して、クライアント端末に記憶しておくようにすれば、単純にファイルや共有鍵を違法コピーしてもコード情報を

10

20

30

40

50

得られなければそのソフトウェアは実行不可能であるため、ソフトウェアの違法コピーにも対処できる。

【0027】(8) ソフトウェア提供者側の装置は、1つのファイルを分割して複数のダウンロード情報として提供する場合には、このファイルのインストール情報に分割に関する情報を含めて送信することもできる。

【0028】こうすれば、例えば大きなファイルの途中でダウンロードしたところで回線が切れたりした場合に、クライアント端末には分割された複数のデータのうち一部が存在することになり、分割された複数のデータのうち存在しない部分だけをダウンロード要求にてサーバに要求することも可能になる。

【0029】(9) 利用者側の装置に設けられた、前記ダウンロード要求を送信するためのプログラム、および、前記ダウンロード情報に従ってインストールを行うためのプログラムのうちの少なくとも一方は、それ自体のバージョン情報を持ち、ソフトウェア提供者側の装置は、複数のインストール情報を送信する際に、利用者側のこれらのプログラムに推奨されるバージョン情報を併せて送信し、利用者側の装置は、前記ダウンロード要求の送信もしくは前記インストールに先立ち、利用者側のこれらのプログラム自身のバージョンアップに必要な情報をソフトウェア提供者に要求するようにしてもよい。

【0030】(10) 本発明は、指定されたソフトウェアをネットワークを介してクライアント端末に提供するサーバ装置(上記ソフトウェア提供者側の装置)であって、クライアント端末から受信したソフトウェア要求により指定されたソフトウェアに対応した複数のファイルのインストール情報を記述したインストールリストを、該クライアント端末がこれら複数のファイルのうち必要なものを選択できるように、該クライアント端末へ送信するインストールリスト送信手段と、クライアント端末が選択した必要なファイルを示すダウンロード要求を受信し、このダウンロード要求に示されるファイルを含むダウンロード情報を、該クライアント端末がこのダウンロード情報に従って該ファイルをインストールできるように、該クライアント端末へ送信するダウンロード情報送信手段とを具備したことを特徴とする。

【0031】(11) 本発明は、ネットワークを介してサーバから提供されたソフトウェアを利用するクライアント装置(上記利用者側の装置)であって、指定するソフトウェアの提供を要求するためのソフトウェア要求を、サーバへ送信するソフトウェア要求送信手段と、このソフトウェア要求の指定するソフトウェアに対応した複数のファイルのインストール情報が記述されたインストールリストをサーバから受信し、この受信したインストールリストを参照して要求すべきファイルを選択し、この選択したファイルを要求するためのダウンロード要求を該サーバへ送信するダウンロード要求送信手段と、このダウンロード要求の示すファイルを含むダウンロー

ド情報をサーバから受信し、この受信したダウンロード情報に従って前記ファイルのインストールを行うダウンロード情報受信手段とを具備したことを特徴とする。

【0032】

【発明の実施の形態】以下、本発明の一実施形態について図面を参照して説明する。図1は、本発明に係るソフトウェア流通方法を用いたソフトウェア流通システムの全体の構成を示したもので、主に、ソフトウェアを販売するサーバ1とソフトウェアを購入するクライアント端末2とを、例えばインターネット等のネットワークを介して接続して構成される。

【0033】図1に示すソフトウェア流通システムは、ソフトウェアを安全かつ簡便に電子的にユーザに配布して、その配布したソフトウェアへの課金を行うシステムである。すなわち、ユーザは、自端末(クライアント端末)2の例えばブラウザでネットワークを介してサーバ1にアクセスし、所望のソフトウェアの購入要求を送信し、サーバ1では、その要求されたソフトウェアをクライアント端末2にダウンロードすると同時に課金を行うもので、ユーザ側では、自端末のマウスを操作するだけでソフトウェアの購入、そのインストールが可能となる。

【0034】さて、図1のソフトウェア流通システムの利用を希望するユーザは、まず、入会ソフトウェアを自端末(例えば、パソコン)2で起動する。入会ソフトウェア(以下、簡単に入会ソフトと呼ぶこともある)は、主に、クライアント端末2にて所定のシステム設定およびサーバ1へのユーザ登録を行うものである。本実施例においてはサーバは1つとして書かれているため、そのサーバにおけるソフトウェア提供者のサイトへの「入会」あるいは「ユーザ登録」として記述しているが、一般には複数のサーバにアクセスすることができる。その場合、利用する各サーバごとに共有鍵を管理することになる。

【0035】入会ソフトは、サーバ1の入会ソフトウェア格納部22に予め格納されており、クライアント端末2からの要求に応じて入会ソフトダウンロード機能部11により、ネットワークを介してクライアント端末2にダウンロードされると同時にクライアント端末2にインストールされる。

【0036】入会ソフトウェア機能部31は、クライアント端末2にインストールされることによりクライアント端末2にて実行可能な状態に設定されて入会ソフトウェアの機能を実行する機能部である。

【0037】なお、入会ソフトは、CD-ROM等の記録媒体にて予めユーザに配布されているものであってもよい。入会ソフトウェア機能部31が起動されると、まず、所定のシステム設定を行う。

【0038】次に、サーバ1へのユーザ登録を行う。まず、サーバ1との間でセキュリティ性の高い情報(例え

ば、クレジットカード番号、認証情報等)を送受信する際に、これらを暗号化・復号化するための鍵データ(セッション鍵、共有鍵等)を生成し、この生成された鍵データに対し所定の暗号化処理を施し、共有鍵は情報ファイル34に格納する。

【0039】さらに、クライアント端末2に表示される手順に従って、ユーザは、自分の氏名、住所、クレジットカード番号、クレジットカードの有効期限、年齢、生年月日等の個人情報等を入力すると、それらは予めサーバ1との間で定められた暗号鍵を用いて暗号化された後、ネットワークを介してサーバ1に送信される。

【0040】サーバ1の入会ソフト受け付け機能部12にて、暗号化された個人情報および鍵データを受信すると、所定の暗号鍵を用いて復号化を行い、信用照会部13を介してカード会社との間で与信照会を行い、与信できた場合はデータベース登録部14を介しての個人情報ファイル24への個人情報および鍵データの書き込み登録処理を終了する。

【0041】ユーザ登録が正常に終了して、その旨の通知を受けたクライアント端末2では、ユーザがソフトウェア購入の際、起動すべきプログラム、すなわち、ダウンロードプログラム35をインストールする。すなわち、ダウンロードプログラム35は、入会ソフトウェアとともにダウンロードされており、それが入会ソフトウェア機能部31から吐き出されて、クライアント端末2にインストールされる。

【0042】ダウンロードプログラム機能部32は、クライアント端末2にインストールされ、メモリ上にローディングされ起動されることによりクライアント端末2にて実行可能な状態に設定されてダウンロードプログラムの機能を実行する機能部である。実行可能な状態においては、ダウンロード要求送信部321およびダウンロード情報受信部322が機能できる。

【0043】入会ソフトウェア機能部31がダウンロードプログラムをインストールする際には、ダウンロードプログラムを自動的に起動するための設定を行う。この設定は、例えば、クライアント端末2で受信したデータのヘッダ部分から、予め定められた識別情報(ここでは、Content-type: Application/ABC)を検知したときにダウンロードプログラムを起動するよう所定のファイルに登録することにより設定がなされる。

【0044】以上で入会ソフトウェアに具備された機能を用いたユーザ登録は終了する。次に、ユーザがサーバ1から所望のソフトウェアをダウンロードする際のソフトウェア流通システムの各機能部について説明する。

【0045】まず、ユーザは、クライアント端末2の例えばブラウザを起動してマウスを操作することによりサーバ1にアクセスして、所望のソフトウェアをリクエストする。具体的には、ソフトウェア要求送信部39がイ

ンストールリスト送信部15に対しソフトウェアの提供の要求を送る。その際、自パソコンに関する環境設定の情報を併せて送信しても良い。

【0046】この送信要求を受けたサーバ1のインストールリスト送信部15では、ユーザにより指定されたソフトウェアに対応するインストールリスト(どのファイルをどのようにインストールするかを記述したリスト)をインストールリスト格納部25から読み出してクライアント端末2に送信する。その際、前記環境設定情報を得た場合には、それに応じてインストールリストを変更して送信する。

【0047】クライアント端末2のダウンロードプログラム機能部は、インストールリストを受信するとダウンロード要求送信部321がそれを処理し、インストールリストに基づき選択された要求(ダウンロード要求)をサーバ1に送信する。インストールリストには、ユーザが要求したソフトウェアに関して、必要なファイル、各々のバージョン、インストール先、サイズ、レジストリへの登録情報、インストール時に実行すべきプログラムなどが書かれていて、それを基に判断する。例えば、既に最新バージョンのファイルを持っていれば、当該ファイルのダウンロード要求を省略する。

【0048】ファイルは持っているがバージョンが古い時にはダウンロード要求が必要であるが、その際、自分の持っているファイルのバージョン情報を送るのが良い。なぜなら、その情報をサーバ側が利用し、最新ファイルを送信するかわりにサイズの小さいパッチ情報を送信することを選択することができるからである。

【0049】サーバ1のダウンロード情報送信部16では、クライアント端末からの要求に応じて、コアソフト格納部26、受動機能ファイル格納部27、ライブラリ格納部28のいずれかからファイルを読み出し、個人情報ファイル格納部24に格納された個人情報を参照して、予め登録されたユーザであることが確認できたら、読み出したファイルをクライアント端末2に送信する。その際、データの圧縮、必要ならばデータの暗号化等を行う。また、クライアント端末2から要求されたファイルが課金対象のものであるときは、個人情報ファイル格納部24に格納された個人情報を参照して、所定の課金処理を行う。

【0050】予め登録されたユーザであることを確認する方法として最も簡単な方法は、予めソフトウェア提供者と利用者として共有された共有鍵を保存しておき、その情報を利用するものであり、これについては後に詳述する。この場合、例えば送信される要求をその共有鍵に関連付けた何らかのチェック、例えば一方向関数を使ったハッシュ値を付けるなどすればよい。これら認証方法については、知られている一般的な方法を用いれば良く、また認証に使う鍵は必ずしも共有鍵である必要も無い。

【0051】クライアント端末2にて実行中のダウンロ

ードプログラムは、ダウンロード情報受信部322がサーバ1からダウンロード情報を受信し、エラーがなければ、インストールする。この際もやはり前述した通り共有鍵を用いるなどして認証を行い、例えば偽のサーバからウイルスを含んだソフトウェアがダウンロードされるような被害を防ぐことができる。

【0052】コアソフト機能部33は、サーバ1からダウンロードされたソフトウェアがクライアント端末2にインストールされることによりクライアント端末2にて実行可能な状態に設定されて所定の情報処理の機能を実現する機能部で、前もってインストールされたコアソフト36が、その起動時に受動機能ファイル37を組み込むことにより正規の機能を呈するようになっている。

【0053】なお、ダウンロードするプログラムはコアソフト、受動機能部以外の汎用のプログラムであってもよく、それは、ライブラリ38としてサーバ1からダウンロードされる。

【0054】インストール済み情報格納部101には、サーバ1からクライアント端末2にダウンロードされて、インストールされたコアソフト36を構成するファイルおよび受動機能部ファイル37に関する情報（ファイル名、バージョン情報、サイズ等）が登録されるようになっている。

【0055】なお、商品としてのソフトウェアは、後述するように、能動機能部ファイルと受動機能部ファイルから構成され、受動機能部ファイルは暗号化されてサーバ1からダウンロードされ、暗号化されたままクライアント端末2に格納される。

【0056】コアソフト機能部33が起動されると、インストール済み情報格納部101を検索して、受動機能部ファイルがインストールされているか否かをチェックする。関連する受動機能部ファイルがインストールされているときは、その暗号化された受動機能部ファイルを復号化して、これを組み込むことにより正規の動作を実行するようになっている。

【0057】次に、図2を参照して、図1のソフトウェア流通システムで用いられる鍵データの流れの一例を説明する。また、必要に応じて、ユーザ登録時のデータの流れの一例を示した図3も参照する。

【0058】入会ソフトウェア機能部31に具備される乱数生成部51は、サーバ1とクライアント端末2にて共有される共有鍵61を乱数で生成する。この共有鍵61は、ソフトウェアの違法コピー防止等に用いられるもので、各クライアント端末2に固有のプロダクトIDを用いて、例えば、DES(Data Encryption Standard)等の秘密鍵暗号化方式で暗号化されて情報ファイル格納部34に鍵ファイル52として格納される。

【0059】また、クライアント端末2にてパスワード62の設定が可能であるならば、そのパスワード62を

共有鍵61を用いてハッシュし、その出力を購入鍵63とする。購入鍵63は、商品(ソフトウェア)購入の際のユーザ認証に用いられるものである。なお、パスワードがないときは、共有鍵61をそのまま購入鍵63としてもよい。

【0060】乱数生成部51は、ユーザ登録時にクライアント端末2でセッション鍵64および共有鍵61を生成する。セッション鍵64は、ユーザ登録時に個人情報および鍵データ(共有鍵61、購入鍵64)を、例えばDES等の秘密鍵暗号方式を用いて暗号化する際に用いられる(図3参照)。このとき、セッション鍵64も、入会ソフトウェアに含まれるソフトウェア販売者との間で予め定められた公開鍵65を用いてRSA(Rivest-Shamir-Adleman)等の公開鍵暗号方式にて暗号化されてサーバ1に送信されるようになっている。

【0061】サーバ1でクライアント端末2から送信された、暗号化された個人情報および鍵データ(共有鍵61、購入鍵63)、セッション鍵を受信すると、まず、暗号化されたセッション鍵64をRSAにて復号化し、この復号化されたセッション鍵64を用いて暗号化された個人情報および鍵データをDESにて復号化する。その後セッション鍵64は廃棄される。

【0062】サーバ1では、復号化された個人情報、鍵データを個人情報ファイル24に保存するとともに、個人情報に基づく信用照会を行うようになっている(図3参照)。

【0063】なお、信用照会の際には、必要に応じて別経路でクライアント端末2に対し再確認を行うようにしてもよい。図4は、個人情報ファイル24に格納される個人情報の記憶例を示したものである。図4に示すように、各ユーザのクライアント端末2から送られてきた鍵データ(共有鍵、購入鍵)とクレジットカード番号、氏名、住所等の個人情報が対応付けされて、ユーザの登録順に記憶されるようになっている。

【0064】個人情報ファイル24に格納された情報は、ここに登録された各ユーザが商品としてのソフトウェアを購入する際のユーザ認証、クレジットカード会社への信用照会とソフトウェアに対する課金処理のために参照される。

【0065】図5は、図1のソフトウェア流通システムで用いられる鍵データの流れと、ユーザがサーバ1から商品ソフトウェアをダウンロードする際のデータの流れを説明するためのものである。

【0066】サーバ1からクライアント端末2へダウンロードされる商品ソフトウェアのうち、コアソフトは、暗号化されておらず、前述したようにクライアント端末にダウンロードと同時にインストールされている。

【0067】一方、受動機能部ファイルをダウンロードする際には、サーバ1では、まず、そのソフトウェアの

10

20

30

40

50

送信要求を行ったユーザの所定の認証処理および課金処理を行った後、そのユーザとの共有鍵61を用いて指定された受動機能部ファイルを暗号化し、クライアント端末2にダウンロードする。

【0068】クライアント端末2では、暗号化された受動機能部ファイルを受信すると、それを所定の領域（暗号化ソフトウェア格納部41（図7参照））に格納する。コアソフトが起動されると、コアソフトは、まず、鍵ファイル52に格納されている暗号化された共有鍵61をプロダクトID67を用いて復号し、復号化された共有鍵61を用いて受動機能部ファイルを復号し、これを組み込む。

【0069】さて、ここで、本実施形態に係るソフトウェア流通システムにてダウンロードされる商品ソフトウェアの特徴について説明する。図6は、商品ソフトウェアの構成を模式的に示したものである。図6に示すように、商品ソフトウェアは大きく分けてコアソフト（能動機能部ファイル）36と受動機能部ファイル37から構成される。

【0070】コアソフト36は、単独で動作可能な無料で提供される、機能・期間限定版のいわゆる試供用のソフトである。受動機能部ファイル37は、ユーザの要求に応じて提供されるもので、すでに配布済みのコアソフト36の期間限定解除、機能追加（バージョンアップを含む）のためのものである。これ単独では動作せず、コアソフトに組み込まれて動作可能となる。

【0071】受動機能部ファイル37は原則有料で、暗号化されてクライアント端末に配布され、クライアント端末では、暗号化されたまま格納されるデータファイルあるいはプログラムファイルである。

【0072】また、コアソフト36は通常複数のファイルから構成され、サイズが大きく、受動機能部は、比較的サイズが小さいものであると考えてよい。図7は、コアソフトの機能を説明するための模式図である。

【0073】コアソフト36は、クライアント端末2にてインストールされても、そのままでは完全には動作しない。これに暗号化された受動機能部ファイル37を復号して追加することによって機能を追加することができる。

【0074】つまり、受動機能部ファイル37を復号する権限のない者が実行しても、全ての機能が動作するわけではない。コアソフト36が起動されるとまず、インストール済み情報格納部101を検索して、そのコアソフトに関連する受動機能部ファイルがインストールされているか否かをチェックする。関連する受動機能部ファイルがインストールされているときは、その暗号化された受動機能部ファイルを暗号化ソフトウェア格納部41から読み出し、ソフトウェア復号部36aにより共有鍵61で復号し、結果として得られた復号受動機能部ファイル37を復号ソフトローディング部36bに格納する。

このとき、もし、共有鍵61を得られない場合は、復号ソフトローディング部36bには正しいデータが格納されない。

【0075】コアソフト36は、ここに配置された受動機能部ファイル37が正しいデータであることを確認する。確認の方法は、例えばここに格納された受動機能部ファイル37が、コアソフトによってあらかじめ予定されたデータに等しい（正しく復号されている）ことをチェックするという方法と、ここに格納された受動機能部ファイル37そのものをプログラムとして実行するという方法が代表的である。

【0076】このように、商品ソフトウェアをコアソフトと受動機能部ファイルに分けて配布することにより次のような利点がある。まず、商品ソフトウェアの有料部分だけを受動機能部ファイルとして販売することができる。例えば、コアソフトは、印刷機能と通信機能が制限されたワードプロセッサであり、印刷機能と通信機能はそれぞれ有料のソフトウェアとして販売される。この方法を用いれば、例えばソフトウェアを購入の都度、サーバ1から送信するのではなく、CD-ROMや電子掲示板のような誰でも入手し参照することが可能な媒体でコアソフトを無料配布しておき、好評ならば有料部分を購入してもらうことができる。

【0077】従来の通信販売の場合、品物が確かめられない制約から、クーリング・オフという制度があるが、形を持たないソフトウェアの場合、一旦購入した物を返品することが不可能である。したがって、コアソフトをまず試供版として顧客に利用してもらうことにより、クーリング・オフのできないことによる顧客の不利益を防ぐことができる。実際に試用した上で、気に入った場合だけ有料の追加機能（受動機能部ファイル）を購入することができる。また、この追加機能は1つだけでなく複数設定することもできるので、「有料」と「無料」の2種類だけでなく、必要な部分だけを適正な価格で買うことができる（不要機能まで抱き合わせ販売されてしまうという不正流通を防げる）。

【0078】次に、暗号化や復号に必要なデータ量が削減できる。一般に、暗号化や復号の計算はデータ量に比例した時間がかかるため、非常に大きなサイズのソフトウェアをその都度暗号化して販売すると、購入（ダウンロード）に時間がかかったり、実行（復号）の際に時間がかかったりするので、暗号化の必要な部分はなるべく小さくする必要がある。

【0079】また、データ量が削減できるということは、通信回線が細くても良いということを意味する。つまり、有料の受動機能部を買うための店舗と顧客との通信回線が遅い場合、一般にはダウンロードに時間を要してしまうが、コアソフトだけはCD-ROMで配布しておいたり、他の高速ネットワークを通じて入手したりしておけば、あとはサイズの小さい暗号化された受動機能

部ファイルだけを入手すれば良く、購入に時間がかからなくなる。

【0080】さらに、違法コピーへの対策としても用いることができる。すなわち、クライアント端末2では、受動機能部ファイルを復号化する際に用いられる共有鍵61は、プロダクトID67によって暗号化保存するという形態を取り、復号された受動機能部ファイルは、コアソフト36が実行される際のメモリ上に存在するだけになるので、単純に、鍵ファイル52、コアソフト36、暗号化された受動機能ファイル37の全てをコピーしても、プロダクトIDを入手しない限り、その違法コピーされたソフトウェアを実行することは不可能となる。また、ソフトウェアの動作メカニズムを解析して違法コピーを作り出すことは難しく、手間をかけてまで違法コピーする価値はなくなる。

【0081】例えば、販売するソフトウェアが書籍である場合、最終的にはメモリ上で計算機等で読める形式の文字列データに変換されてしまうため、そのデータをメモリ上から盗み読むことは比較的簡単にできてしまう。しかし、コアソフト36は「書籍を読むソフト」としておき、有料の追加機能である個々のソフト（書籍）を受動機能部ファイルとして読み込んで、その内容を画面に表示するという仕組みにしておくことができる。この場合、コアソフト36が必要なデータ（暗号化されたデータ）を随時復号して表示する仕組みにすれば、書籍のデータ（文字）全部をまとめて読み出すというのは非常に困難になる。

【0082】また、復号された受動機能部ファイルは、コアソフト36が実行される際のメモリ上に存在するだけになるので、コアソフト36が暗号化ソフトウェアを利用する方法手順を煩雑にすることによって、販売されたソフトウェアの暗号を解く手間が非常に大きくなり、安全性が高まる。

【0083】一般に、ネットワークで販売されるソフトウェアは、バージョンアップが比較的頻繁であったり、一時的にしか価値のない情報（例えば天気予報）のようなものである場合が多く、ソフトウェアの違法コピー作成に知恵を絞るよりも、正しくお金を払ってソフトウェアを購入した方がはるかにコストが安くなるため、違法行為を行う意味がなくなり、ソフトウェアの公正な流通が促進される。

【0084】次に、図8を参照して、ユーザがサーバ1から所望のソフトウェアをダウンロードする際のより詳細な処理手順、すなわち、ダウンロードプログラム機能部32の処理手順について説明する。

【0085】ユーザは、クライアント端末2の例えばブラウザを起動してマウスを操作することによりサーバ1にアクセスして、サーバ1に対し所望のソフトウェアをリクエストする。このとき、クライアント端末2にて予め実行された環境自動判定結果の内容を記述したファイ

ルもサーバ1に送信される（ステップS1）。

【0086】この送信要求を受けたサーバ1のインストールリスト送信部15では、ユーザにより指定されたソフトウェアに対応するインストールリスト（どのファイルをどのようにインストールするかを記述したリスト）をインストールリスト格納部25から読み出してクライアント端末2に送信する（ステップS2）。

【0087】図9は、サーバ1から送信されるデータ構成例を示したもので、主に、ヘッダ部とデータ部から構成される。ヘッダ部には、識別情報71（Content-type: Application/ABC）を含み、クライアント端末2で、この識別情報71を検知するとダウンロードプログラムを自動的に起動するようになっている（この設定は、入会ソフトウェア機能部31がダウンロードプログラムをインストールする際になされている）。

【0088】データ部には、ここでは例えばインストールリストが挿入されている。図9に示すように、インストールリストには、ダウンロードプログラムの最新バージョン（Download-version）、サーバ1のアドレス情報（例えば、URL）、複数の「命令」から構成される。

【0089】この「命令」は、ユーザがマウスをクリックした際に、何の機能を選択したのかをダウンロードプログラムに知らせるためのもので、例えば、図10に示すように、どのファイルをどのようにインストールするかを記述した（コアソフトあるいは受動機能の）インストール命令がある。図11に図10に示したインストール命令の具体例を示す。

【0090】図11に示したインストール命令の意味は、「ファイル名:MTのversion1のdic2機能のRevision3が必要で、これを3個に分割して送信する。1個目と2個目の送信量は512Kバイトで3個目の送信量は139Kバイトである。3つのファイルを連結した後に圧縮の解凍をすると7439Kバイトのファイルになる。」である。このように、図10に示したインストール命令によりソフトウェアの分割ダウンロードが可能となる。なお、図10の分割指定のフィールドにおいて、 $n=1$ とすれば一括ダウンロードの指定も可能である。

【0091】分割ダウンロードが指定された場合には、各分割データごとに繰り返しサーバにダウンロードを要求する。その際、何番目のデータを要求するのかサーバに対し指定する。例えば、ファイル名に一定の規則の拡張子（例えば、_PART1、_PART2）を付けることによって表現できる。

【0092】「命令」には、図10に示したようなインストール命令の他に、例えば、「ユーザの購入済みソフトのバージョンアップ情報の表示」命令もある。この命令は、この命令文内で指定されたファイルがインストー

10

20

30

40

50

ルされていないときは、以下のインストール命令の実行をエラーとするもので、これは、受動機能部を販売する際には、必ずそれに対応するコアソフトがインストールされて正常に動作していることを確認するためのものである。

【0093】また、この「命令」は、「このプログラムを実行した結果がこの値ならばこのインストールを行う」といった条件式であっても良い。その際に動かすプログラム自体がインストール命令に書かれていれば、「まずこのプログラムをダウンロードし、それを動かした結果によってこのインストールを行う」という動作が可能なので、こういった複雑なインストール条件が、単純な「命令」の組合わせで実現できる。

【0094】例えば、「Install checkprogram 100 230」という命令に続き、「IF checkprogram 0 Install DIC MT/1/dic8.3 100400」という命令の書かれているインストールリストを用いれば、「checkprogramという名前のプログラムをまずダウンロードし、しかる後にそのプログラムを実行し、その結果の値が0であったらDICをインストールする」という複雑なインストール指定を行うことも容易にできる。

【0095】さて、ステップS2で、クライアント端末2がサーバ1からインストールリストを受け取ると、図9のヘッダ部に含まれる識別情報71を検知し、ダウンロードプログラムを起動する。そして、受信したインストールリストに含まれるダウンロードプログラムの最新バージョン(Download-version)をチェックする(ステップS3)。新しくなっていたら、最新のダウンロードプログラムのダウンロードをサーバ1に要求する(ステップS4)。サーバ1は、所定のソフトウェア格納部から最新版のダウンロードプログラムのファイルを読み出して、暗号化せずにクライアント端末2にダウンロードする(ステップS5)。

【0096】クライアント端末2で、最新版のダウンロードプログラムのファイルを受け取ると、他のファイルのダウンロードとは別に扱う。すなわち、現在実行中のダウンロードプログラムに上書きすることはなく、例えば、現在実行中のダウンロードプログラムが「download1」の名前でインストールされているならば、最新版のダウンロードプログラムを「download2」の名前でインストールし、さらに、ダウンロードプログラムの自動実行するための設定ファイルの書き換えも行う。その後、現在実行中のダウンロードプログラム「download1」で処理中のデータをそのまま最新版のダウンロードプログラム「download2」に渡して、最新版のダウンロードプログラムを起動する。従って、バージョンアップ後は常に「download1」と「download2」の2つのプログラム

ファイルが存在することになる。

【0097】このように、最新版のダウンロードプログラムのバージョンアップを他のファイルのダウンロードとは別に扱う理由は、現在実行中のダウンロードプログラムに新しいファイルを上書きしても現在実行中のダウンロードプログラムの実行内容が新しくなるわけではないからである。

【0098】次に、クライアント端末2では、インストールリストに記述された、先にユーザにより指定されたソフトウェアを構成するファイル(コアソフト、受動機能部ファイル)のバージョン情報とインストール済み情報格納部101に登録されているファイルのバージョン情報とを比較し、バージョンアップされているファイルがあるか否か、あるいは、インストールリストに新たな追加機能ファイル(受動機能部ファイル)が存在するか否か等をチェックして、そのようなファイルが存在する場合には、必要なファイルに関してサーバ1に所定のヘッダ情報を付けたダウンロード要求を出す(ステップS6)。

【0099】ダウンロード要求には、例えば、現在インストールされているファイルのバージョン等の情報も含まれている。また、ヘッダ情報には、ユーザ登録済みである旨を示す各種情報(例えば、購入鍵等)が含まれている。

【0100】サーバ1は、クライアント端末2からのダウンロード要求を受け取り、そのヘッダ情報からユーザ登録済みのユーザであることを認識すると、ダウンロード要求の処理を実行し、図12に示すようなフォーマットにて、指定されたファイルのダウンロードを行う(ステップS7)。

【0101】その際、ダウンロード要求された情報が有料のものである場合には、必要な課金処理を行う。その際、共有鍵はソフトウェア利用者のソフトウェア料金の決済に関わる識別情報との対応付けが入会手続き時に保証されているので、その識別情報を利用して課金を行うのが普通である。さらに、予め暗号化するものと指定された有料の受動機能である場合には共有鍵によってその暗号化も行う。

【0102】図12において、送信フォーマットのフィールドには送信されるデータの種別が記述される。例えば、「0」はファイル全体を一括して送る、「1」はデータの差分を一括して送る、「2」は分割ダウンロードで全体を送る、「3」は分割ダウンロードでデータの差分を送る、である。

【0103】データ本体のフィールドに挿入されるファイルは、所定の圧縮プログラムにより圧縮されていてもよい。このとき、その解凍プログラムはダウンロードプログラムに含まれていてもよいし、外部のプログラムを読み込むようにしてもよい。

【0104】データサイズはデータ本体のサイズ、MA

SKは、復号時に共有鍵にかけるマスク、checksumは、データ本体（暗号化していないもの）に対するチェックサム、ハッシュ値は、データサイズ、データ本体、checksum、MASKの全体にハッシュ関数をかけたものである。ハッシュ値が正しくなければダウンロードプログラムはエラーを検知するようになっている。なお、MASKが「0」のとき、このフォーマットのデータ本体であるファイルは暗号化対象でないことを意味する。

【0105】このように、ダウンロード情報を共有鍵に関連付けておくことにより、正規のサーバ（すなわち自分の共有鍵を知っているサーバ）からのダウンロード情報であることを確認することができ、ウイルスが入り込むなどの不正なインストールが防ぎやすくなる。

【0106】サーバ1では、ファイルの送出後、そのファイルが有料である場合は、購入鍵をキーに個人情報ファイル24を参照して、そのユーザのクレジットカード番号を取得し、それを基にクレジットカード会社との間で信用照会および課金処理を行う。

【0107】また、ダウンロードの際に、暗号化を要する部分は予め登録された共有鍵で暗号化する。なお、課金されたがダウンロードの途中で失敗（回線が切れた等）した場合は、そのまま無視する。そのユーザが再度購入操作をしたとき課金処理を行うことなくダウンロードやり直すだけである。

【0108】以上、説明したように、本実施形態に係るソフトウェア流通システムの効果を以下にまとめる。

(1) 自動インストール機能

クライアント端末2における環境自動判定結果をサーバ1に送信し、サーバ1は、それに応じたソフトウェアを配布し、クライアント端末2においてダウンロードプログラムに具備されるインストーラにてダウンロードされたファイルを受け取ると同時にインストールする。これにより、パソコンの知識がなくとも簡単にかつ間違いなくインストールすることが可能となる。

【0109】また、サーバ1からダウンロードされるファイルを自動インストールする際には、クライアント端末2のダウンロードプログラムは、ユーザ登録時に設定された識別情報を認識して処理を実行することにより、ウイルスの入り込む心配がない。

(2) 自動課金機能

ユーザ登録時にクレジットカード番号等をサーバ1に登録することにより、ソフト購入時には、所望するソフトウェアの購入要求のみを送信すれば、後はサーバ1にて、その登録されたクレジットカード番号を用いてオンライン信用照会により、即時課金を行う。従って、ユーザは、マウスのクリックだけでソフトウェアの購入ができるため、安価なソフトウェアの販売にも向いている。購入の都度クレジットカードの番号を入力することもないので、安全性が高くなる。

【0110】また、本発明の手順によれば、ユーザは実際に必要な（持っていない）情報のみをダウンロード要求するため、既に持っている情報に関して二重に課金されることは起らない。従来のシステムにおいては、例えば初回のダウンロード時に課金ログをサーバ側に生成し、2回目以降はその課金ログを元に非課金とするとといった煩雑なチェックが必要であった。

(3) 自動バージョンアップ機能

ダウンロードプログラムは、サーバ1から送信されるインストールリストを参照して、自端末にインストール済みのファイルがバージョンアップされているか否かをチェックし、その結果をユーザに提示する。ユーザはこれをもとに必要なファイルのダウンロード要求をマウス等を操作するだけで簡単行える。しかも、必要な部分のみサーバ1からダウンロードされるわけであるから通信量が少なく回線費用が割安となる。

(4) ソフトウェアの試供

まず、無料の試供版ソフト（コアソフト）を試用した後、それに付加して正規の動作が可能となる課金対象部分のソフト（受動機能部）を購入する仕組みなので、購入した製品のトラブルや不満が無くなり、返品が不可能な電子的情報の販売に向いている。

(5) 違法コピー防止機能

課金対象部分のソフト（受動機能部）は、サーバからダウンロードされてクライアント端末にインストールされる際に暗号化されたまま格納され、ソフトの起動時の度にコアソフトの復号化組込機能にて受動機能部ファイルが復号化されて実行可能なように変換される。そして、その復号化の際に用いられるユーザ固有の共有鍵は、クライアント端末に一義的に定められるプロダクトIDにて暗号化されて格納されている。従って、単純に、鍵ファイル52、コアソフト36、暗号化された受動機能部ファイル37の全てを違法にコピーしても、プロダクトIDを入手しない限り、その違法コピーされたソフトウェアを実行することは不可能となる。

(6) ダウンロードプログラムのバージョンアップ

クライアント端末2のダウンロードプログラムでは、サーバ1から送信されるインストールリストに記述されるダウンロードプログラムのバージョン情報をチェックし、新しくなっていたら最新のダウンロードプログラムのダウンロードを自動的にサーバ1に要求することにより、ダウンロードプログラムのバージョンアップが容易に行え、従って、インストールリストに記述される命令の種類追加等が容易となる。

(7) ソフトウェアの分割ダウンロード

サイズの大きいソフトウェアをダウンロードする際には、分割してダウンロードすることを指定した命令を、インストールリストに含めることにより、その旨をクライアント端末2に通知することができゆえに分割ダウンロードが可能となる。

【0111】これにより、ダウンロード時にサーバ1とクライアント端末2との間の通信回線に障害が発生して、正常にダウンロードできなくとも、再度マウスのクリック等の簡単な操作により、ダウンロードを継続することができる。

【0112】また、インターネット上では1セッションの通信サイズが制限される場合があるが、そのようなネットワークにおいても、分割ダウンロードを利用することにより、どんなにサイズの大きな情報でも確実に送信することができる。

【0113】なお、上記実施形態において、受動機能部は課金対象のソフトウェアとして説明したが、この場合に限らず、能動機能部への無料の追加機能としても同様に実現することができる。従って、この場合は受動機能部の暗号化は必ずしも行う必要はない。

【0114】

【発明の効果】本発明によれば、ソフトウェア提供者がソフトウェアのインストールにかかわるインストールリストを予め送信し、それを利用者のパソコン等でダウンロードする前に解釈する手順を踏むことにより、ソフトウェアのインストールに際して実際に必要なデータだけを効率良くしかも自動的に転送しインストールすることができるため、簡易な操作でネットワークを介したソフトウェアの流通が可能となる。

【0115】また、必要なデータだけ送ることは、単に送信データ量が少なくなるだけでなく、各データそのものに価格を設定することができるため、ソフトウェアの提供の際に柔軟な課金を行うことができる。

【図面の簡単な説明】

【図1】本発明の実施形態に係るソフトウェア流通システムの全体の構成図。

【図2】図1のソフトウェア流通システムで用いられる

鍵データの流れを説明するための図。

【図3】ユーザ登録時のデータの流れを説明するための図。

【図4】個人情報ファイルに格納される個人情報の記憶例を示した図。

【図5】図1のソフトウェア流通システムで用いられる鍵データの流れと、ユーザがサーバから商品ソフトウェアをダウンロードする際のデータの流れを説明するための図。

10 【図6】商品ソフトウェアの構成を模式的に示した図。

【図7】コアソフトの機能を説明するための図。

【図8】ダウンロードプログラム機能部の処理手順について説明するための図。

【図9】サーバから送信されるデータの構成例を示した図。

【図10】インストールリストに記述されるインストール命令の一例を示した図。

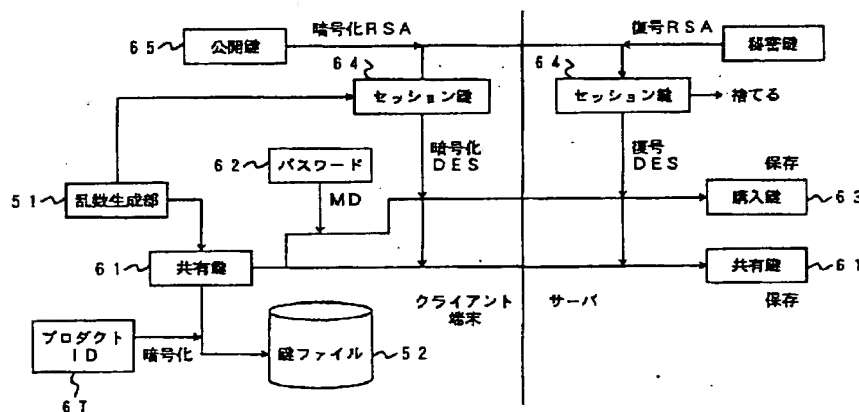
【図11】図10のインストール命令の具体例を示した図。

20 【図12】ダウンロードデータの構成例を示した図。

【符号の説明】

- 1…サーバ
- 2…クライアント端末
- 11…入会ソフトダウンロード機能部
- 12…入会ソフト受け付け機能部
- 15…インストールリスト送信部
- 16…ダウンロード情報送信部
- 31…入会ソフトウェア機能部
- 32…ダウンロードプログラム機能部
- 33…コアソフト機能部
- 36…コアソフト
- 37…受動機能ファイル

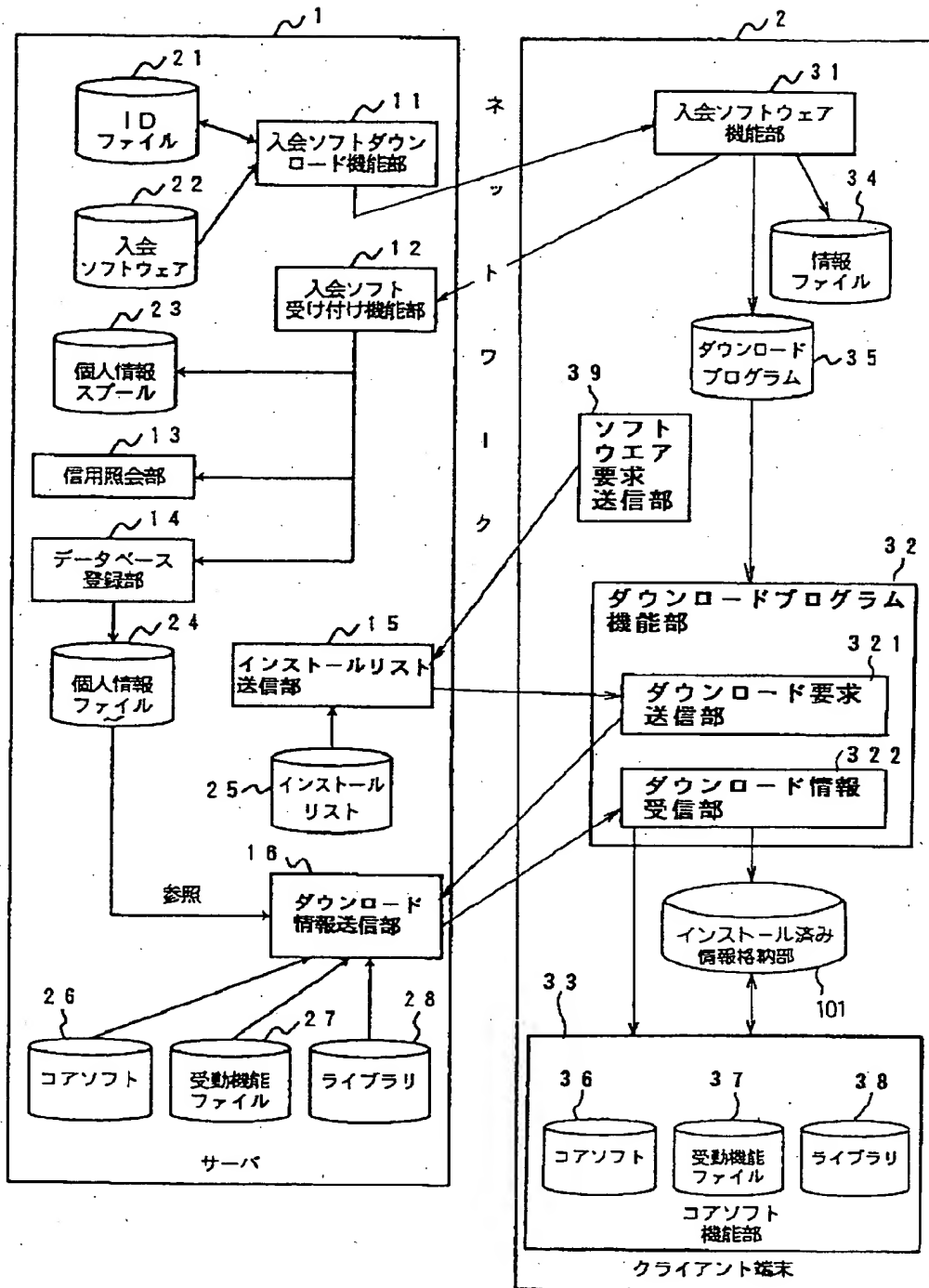
【図2】



【図12】

送信フォーマット (1 byte)
データ・サイズ (4 byte)
データ本体 (一部暗号化されている場合 もある)
check sum (32 bit)
MASK (128 bit)
ハッシュ値

【図1】



【図10】

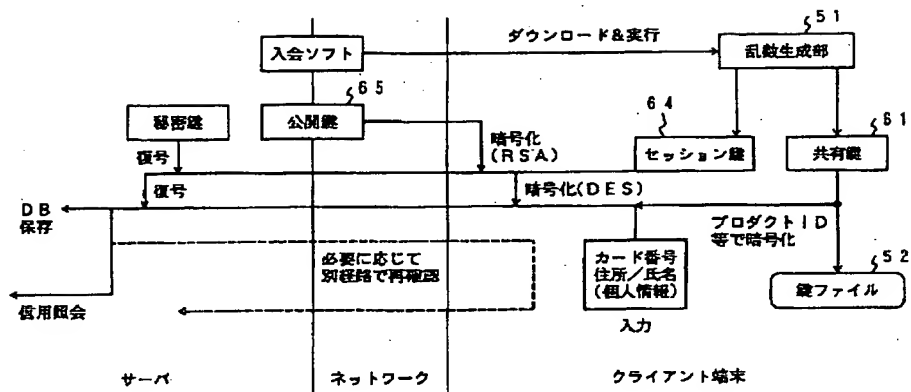
【図11】

```
Install funcname pathname size1-1 size1-2 .. size1-n size2
```

命令種別 ファイルの指定 分割指定 ファイルの全容量

```
Install DIC MT/1/dic2.3.ep1 512000 512000 139000 7439000
```

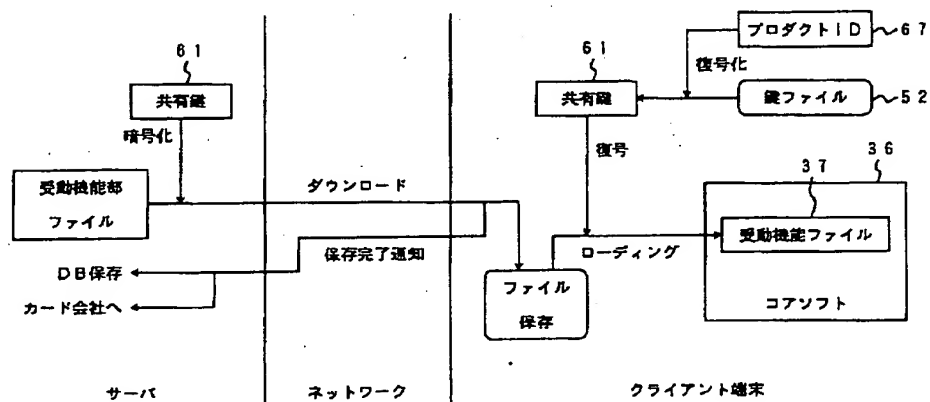
【图 3】



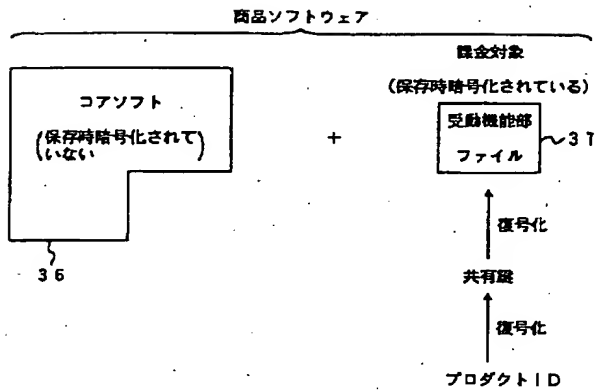
【图 4】

個人情報				
登録順	共有鍵	購入歴	クレジットカード番号	個人情報
1	3425608	6827641	22-52-6643	山田太郎 〒100 港区…
2	2162430	3287621	21-66-3225	山田花子 〒144 横岡県…
3	3352762	5582387	44-32-2152	鈴木一郎 〒200 港区…
4	4626187	—	—	—
5	8613215	8903214	—	佐藤二郎 〒300 秋田県…
6	4892314	2292362	21-62-3315	高橋一郎 〒146 大田区…
7	4452361	6473219	33-25-4111	前田 浩 〒300 秋田県…
⋮				

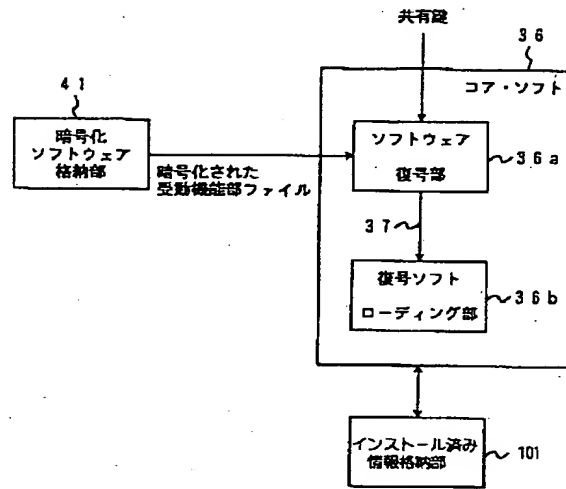
【图 5】



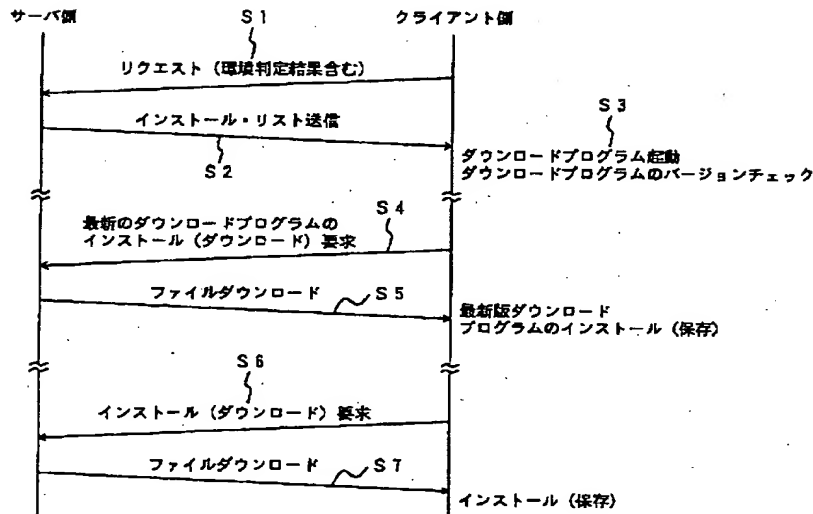
【図6】



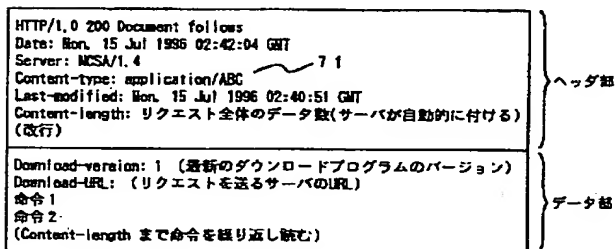
【図7】



【図8】



【図9】



フロントページの続き

(51) Int. Cl.⁶

識別記号

F I

G 0 6 F 17/60

G 0 6 F 15/21

Z